UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

JANE DOE, *individually and on behalf of all others similarly situated*, Plaintiff, v. **THE KROGER CO.**, Defendant.	Case No. 1:23-cv-00741 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jane Doe ("Plaintiff"), individually and on behalf of all others similarly situated, hereby files this class action complaint against Defendant The Kroger Co. ("Defendant" or "Kroger"), and in support thereof alleges the following:

INTRODUCTION

1. Plaintiff brings this class action against Kroger to address Defendant's unlawful practice of disclosing Plaintiff's and Class Members' confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information") to unauthorized third parties via tracking technologies and analytics software embedded on its website ("Tracking Tools"), including Meta Platforms, Inc.'s Tracking Pixel (the "Meta Pixel" or "Pixel").

2. Unbeknownst to patients, Defendant installed these and other Tracking Tools on its Website, Kroger.com, which surreptitiously manipulated their web browsers, thereby causing their communications with the Defendant via the Website ("Communications") to be shared and/or intercepted by unauthorized third parties.

3. Plaintiff and Class Members used the Website to submit information related to their prescriptions. The Private Information unauthorized third parties received revealed individual patients' identities and details about the confidential health care they sought and received from Defendant, including the name of their prescription medications, dosage and form of the medication, and more. In turn, these disclosures allow third parties to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy, HIV, mental health conditions, and an array of other symptoms or conditions.

4. The information collected and disclosed by Defendant's Tracking Tools is not anonymous. Facebook connects user data from Defendant's Website to the individual's Facebook ID ("FID"). The FID links the user to his/her Facebook profile, which contains detailed information about the profile owner's identity.

5. Simply put, the health information disclosed through the Tracking Tools is personally identifiable.

6. Information about a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of such information can have serious consequences, including discrimination in the workplace or denial of insurance coverage.

7. Under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), pharmacies such as Defendant's are "covered entities" and are required to follow strict rules regarding the use and disclosure of individuals' health information.[1]

[1] 42 U.S.C. § 1320d; 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164. Defendant is engaged in the sale and dispensing of drugs in accordance with prescriptions, and therefore qualifies as a "person or organization who furnishes, bills, or is paid for health care." *Id.*

8. The United States Department of Health and Human Services (HHS) has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the HIPAA "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the Privacy Rule, no health care provider – including pharmacies like Defendant – can disclose a person's personally identifiable protected health information to a third party without express written authorization.

9. In addition, as explained further below, HHS has specifically warned healthcare regulated entities—such as Defendant—that tracking technologies like the ones used on its Website transmit personally identifying information to third parties, and that such information should not be transmitted without a HIPAA-compliant written authorization from patients.

10. The Federal Trade Commission (FTC) has also warned hospitals and other entities that "even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule." [2, 3]

---

[2] On February 1, 2023, the U.S. District Court for the Northern District of California entered a Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief in *USA v. GoodRx Holdings, Inc.*, Case No. 3:23-cv-00460 (Doc. 3-1), which addressed the same misconduct at issue here against Kroger.

[3] The FTC further clarified that entities who are not covered by HIPAA are nonetheless required to obtain affirmative express consent prior to disclosing health information, which is defined as: "any freely given, specific, informed, and unambiguous indication of an individual's wishes demonstrating agreement by the individual, such as by a clear affirmative action, following a Clear and Conspicuous disclosure to the individual, apart from any 'privacy policy,' 'terms of service,' 'terms of use,' or other similar document, of all information material to the provision of consent. Acceptance of a general or broad terms of use or similar document that contains descriptions of agreement by the individual along with other, unrelated information, does not constitute Affirmative Express Consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute Affirmative Express Consent. Likewise, agreement obtained through use of a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, does not constitute Affirmative Express Consent." *U.S.A. v. Easy Healthcare Corp. d/b/a Easy Healthcare* (N.D. Ill 2023), Stipulated Settlement accessible online https://www.ftc.gov/system/files/ftc_gov/pdf/2023.06.22_easy_healthcare_signed_order_2023.pdf (last access Nov. 10, 2023).

11. Ohio state law, including Ohio Revised Code § 3798 *et al*., ["Ohio Protected Health Information"], expressly prohibits the disclosure of Private Information without express written authorization.

12. Despite these clear laws and regulations, Defendant has essentially planted a bug on patients' web browsers that forced them disclose private and confidential Communications to third parties. Kroger's utilization of the Tracking Tools to secretly track and share with third parties its users' Communications on its Website is the electronic equivalent of looking over the shoulder of each visitor for the entire duration of their Website interaction. Defendant did not disclose the presence of these Tracking Tools to Website users filling prescriptions with Kroger.

13. Patients simply do not anticipate or expect that their trusted healthcare provider will send personal health information or confidential medical information regarding their prescriptions to a hidden third party—let alone social media networks and online advertisers like Facebook which have sordid histories of privacy violations in pursuit of ever-increasing advertising revenue—without patient consent. Patients did not sign a written authorization permitting Defendant to send their Private Information to Facebook, and Defendant does not have a HIPAA-compliant business associate agreement with Facebook.

14. Defendant breached its statutory and common law obligations to its patients by, inter alia,: (i) failing to remove or disengage technology that was known and designed to share patients Private Information, including sensitive details such as the exact name of their prescription medications; (ii) failing to obtain the written consent of patients to disclose their Private Information to Facebook and any other unauthorized third parties with whom Defendant has failed to execute a HIPAA-compliant business associate agreement; (iii) failing to take steps to block the transmission of patients' Private Information via Tracking Tools on its Website; (iv) failing to warn

patients; and (v) otherwise failing to design, and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

15. Plaintiff is an adult citizen of Ohio, and brings this action individually and on behalf of a nationwide class consisting of consumers whose Website Communications were surveilled in real-time and intercepted through Defendant's procurement and use of the Tracking Tools embedded on the webpages of www.kroger.com, causing them injuries, including (i) invasion of privacy; (ii) loss of benefit of the bargain, (iii) diminution of value of the Private Information, (iv) statutory damages, and (v) the continued and ongoing risk to their Private Information (collectively, the "Class").

16. Plaintiff and putative Class Members seek all civil remedies provided under the causes of action listed below, including but not limited to compensatory, statutory, and punitive damages, and attorneys' fees and costs.

17. Plaintiff and putative Class Members seek injunctive relief that will halt Defendant's ongoing unlawful conduct.

THE PARTIES

18. Plaintiff Jane Doe is a citizen of the State of Ohio, and at all times relevant to this action, resided and was domiciled in Hamilton County, Ohio, and visited and utilized the Kroger Website.

19. Class Members are adult U.S. citizens who are patients and/or individuals who visited Kroger's Website from their computers and/or mobile devices and used the Website to order prescriptions or schedule appointments. At all relevant times, putative Class Members maintained accounts with Facebook, or the other third parties to whom Defendant disclosed Private Information. During the relevant time period, putative Class Members visited Kroger's Website to

search for personal, health-related products and information, pharmacy-related products and information, and medications.

20. Defendant, The Kroger Co., is a public company with its principal place of business at 1014 Vine Street, Cincinnati, Ohio 45202. Kroger is one of the largest supermarket operators in the United States. Kroger employs approximately 465,000 individuals nationwide and generated annual revenue in the amount of $3.477 billion in 2022.[4] Its Website facilitates consumer searches for medications and discounts on those medications, as well as research regarding symptoms, illnesses and health conditions, vaccine information, and scheduling telehealth appointments with licensed healthcare providers.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all putative Class Members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more Members of the proposed Class, and at least one Member of the proposed Class is a citizen of states different than Defendant.

22. This Court has personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in Ohio, where Defendant maintains its corporate headquarters. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of Ohio while they were located within Ohio. At all relevant times, Defendant knew that its practices would directly result in the real-time viewing and collecting of information from Ohio citizens while those citizens browse www.kroger.com. Defendant chose to avail itself of the business opportunities of marketing and

[4] https://www.wsj.com/market-data/quotes/KR/financials/annual/income-statement

selling its services in Ohio and viewing real-time data from Website visit sessions initiated by Ohio citizens while located in Ohio, and the claims alleged herein arise from those activities.

23. Defendant also knows that many Website users visit and interact with Defendant's Website while they are physically present in Ohio. Defendant's Website allows users to search for nearby stores by providing the user's "current location," as furnished by the location-determining tools of the device the user is using or by the user's IP address (i.e., without requiring the user to manually input an address). Users' employment of automatic location services in this way means that Defendant is continuously made aware that its Website is being visited by users located in Ohio, and that such Website visitors are being wiretapped in violation of Ohio statutory and common law.

24. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

Website User and Usage Data Have Immense Economic Value

25. The "world's most valuable resource is no longer oil, but data."[5]

26. Recently, Business News Daily reported that some businesses collect personal data (i.e., gender, web browser cookies, IP addresses, and device IDs), engagement data (i.e., how consumers interact with a business's website, applications, and emails), behavioral data (i.e., customers' purchase histories and product usage information), and attitudinal data (i.e., data on

[5] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data.

consumer satisfaction) from consumers.[6] This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.[7]

27. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations that "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[8]

28. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[9] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[10]

29. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e., $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military are estimated to cost USD 55."[11]

---

[6] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing with It)*, Business News Daily (updated Aug. 25, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

[7] *Id.*

[8] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.

[9] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.

[10] *Id.* at 25.

[11] *Id.*

Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites.

30. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that "a full 86% of the Defendants said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected."[12]

31. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.[13] As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[14]

32. Privacy polls and studies show that most Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

33. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[15]

---

[12] Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/.

[13] *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html.

[14] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, The Information Society, 38:4, 257, 258 (2022).

[15] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds,* Consumer Reports (May 11,2017) https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/

34. Moreover, according to a study by Pew Research Center, most Americans, approximately 79%, are concerned about how data is collected about them by companies.[16]

35. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.[17]

Ohio Revised Code § 2933, et seq.

36. Ohio Revised Code § 2933 provides for a civil cause of action for any person whose wire, oral, or electronic communications are intercepted, disclosed, or intentionally used in violation of §§ 2933.51 to 2933.66 of the Revised Code. Available relief for such violations may include the preliminary and other equitable or declaratory relief that is appropriate; Whichever of the following is greater: (1) Liquidated damages computed at a rate of two hundred dollars per day for each day of violation or (2) liquidated damages of ten thousand dollars, whichever is greater; The sum of actual damages suffered by the plaintiff and the profits, if any, made as a result of the violation by the person or entity that engaged in the violation; Punitive damages, if appropriate; and reasonable attorney's fees and other litigation expenses that are reasonably incurred in bringing the civil action.

37. To establish liability under Ohio Revised Code § 2933, Plaintiff and putative Ohio Class Members need only establish that the Defendant caused a wrongful intrusion into one's

---

[16] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-Confusedand-feeling-lack-of-control-over-their-personal-information/.

[17] Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

private activities in such a manner as to outrage or cause mental suffering, shame, or humiliation to a person of ordinary sensibilities.

Electronic Communications Privacy Act ("ECPA")

38. The ECPA prohibits the intentional interception of the contents of any electronic communication. 18 U.S.C. § 2511. The elements of an ECPA claim are:

> (1) Except as otherwise specifically provided in this chapter any person who—
>
> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or
>
> shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

18 U.S.C. § 2511 (1)(a) and (c)-(d). As discussed below, Plaintiff and putative Class Members satisfy each of these elements.

Defendant's Website and the Tracking Tools Employed by Defendant for the Purpose of Disclosing Plaintiff's and Class Members' Private Information to Third Parties.

39. Defendant's Website, www.kroger.com, is accessible on mobile devices and desktop computers and gives users the option to search for and obtain information about

prescription drugs, including discounts on those drugs, as well as symptoms, illnesses and health conditions, and to schedule telehealth appointments and/or vaccinations.

40. In order to use Defendant's Website, patients must provide Defendant with certain sensitive and personal information. For example, when ordering or refilling prescriptions, patients must create an account, including their first and last name and email address, and enter the names of the prescription medications they are ordering. These medications are often clearly associated with a particular medical condition or disease.

41. Similarly, when looking for discounts on prescription drugs, patients must enter the names of their prescription medications and their locations. If patients do not specify their location, the Website independently determines users' locations. And when scheduling telehealth appointments, patients must provide their email addresses, phone numbers, dates of birth, biological sex, mailing address, and identify their specific, sensitive, and private health issues, such as depression, a urinary tract infection, or erectile dysfunction.

42. As a result, patients share and communicate Private Information, including PII and/or PHI, with Defendant via its Website.

43. Defendant purposely installed the Tracking Tools on its Website and programmed specific webpage(s) to surreptitiously share its patients' Private Information with third parties, including Meta.

44. The Tracking Tools track patients as they navigate through the Website and transmit to third parties each patient's Communications, including specific information patients enter into search bars and text boxes regarding their prescriptions and requests for vaccination or other appointments.

45. The Tracking Tools also capture patients' IP addresses. An IP address is a unique number assigned to a user's internet-enabled device that informs websites of the device's city, zip code, and physical location.

46. Notably, after patients provide their Private Information via Defendant's Website, Kroger, without the patients' knowledge or consent, supplies this Private Information to third parties such as Meta via the Tracking Tools. Plaintiff and putative Class Members did not and could not anticipate that Defendant would aid and conspire with Meta, and other third parties to intercept and transmit their Communications, which include Private Information.

47. If the patient is also a Facebook user, the Private Information that Meta receives from Defendant is linked to the user's Facebook profile (via their Facebook ID or "c_user id"), which includes other identifying information, including the identity of the person that is transmitting the Private Information.

48. However, patients who provided their Private Information, as described above, were not notified by Kroger's Privacy Policy or Notice of Privacy Practices or about its use of the Tracking Tools, or that their Private Information would be shared with third parties.

Meta's Business Tools and the Pixel

49. Meta operates the world's largest social media company and generated $116 billion in revenue in 2022, roughly 98% of which was derived from selling advertising space.[18]

50. In conjunction with its advertising business, Meta encourages and promotes entities and website owners, such as Defendant, to utilize its "Business Tools" to gather, identify, target, and market products and services to individuals.

[18] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx

51. Meta's Business Tools, including the Pixel, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of website visitors' activity.

52. The Business Tools are automatically configured to capture "Standard Events," such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.[19] Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[20]

53. One such Business Tool is the Pixel, which "tracks the people and type of actions they take."[21] When a user accesses websites hosting the Pixel, Private Information provided to the host website is surreptitiously sent to Meta. Notably, this transmission does not occur unless the website contains the Meta Pixel. Stated differently, each putative Class Member's Private Information would not have been disclosed to Meta but for Defendant's decisions to install the Pixel on its Website.

54. As explained in more detail below, this secret transmission is initiated by Defendant's source code to share Plaintiff and Class Members' Private Information, which was intended exclusively for Defendant, with Meta.

---

[19] FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (last visited Sep. 1, 2023); *see* FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Sep. 1, 2023).

[20] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBPAGE(S) EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/. (last visited last visited Sep. 1, 2023)

[21] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

Defendant's Use of the Tracking Tools

55. Web browsers are software applications that allow users to navigate the internet and exchange electronic communications, and every "client device" (computer, tablet, or smart phone) has a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

56. Correspondingly, every website is hosted by a computer "server," which allows the website's owner (Defendant) to exchange communications with the website's users (Plaintiff and Class Members) via the users' web browser.

57. When a user visits Defendant's Website and undertakes various actions, the user and Defendant are engaged in an ongoing back-and-forth exchange of electronic communications taking place via the user's web browser and Defendant's computer server.

58. These communications are invisible to ordinary users because they consist of HTTP Requests and HTTP Responses, and one browsing session may consist of thousands of individual HTTP Requests and HTTP Responses.[22]

> **HTTP Request:** an electronic communication sent from the website visitor's browser to the website's corresponding server. In addition to specifying a particular URL (i.e., web address), "GET" HTTP Requests can also send data to the host server, including cookies. A cookie is a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Some cookies are "third-party cookies" which means they can store and communicate data when visiting one website to an entirely different website.
>
> **HTTP Response:** an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a

[22] See HHS Bulletin § *What is a tracking technology?* ("Tracking technologies collect information and track users in various ways, many of which are not apparent to the website or mobile app user.")

> web page, another kind of file, text information, or error codes, among other data.

59. A user's HTTP Request essentially asks Defendant's Website to retrieve certain information, and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the user's screen as they navigate Defendant's Website).

60. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website user's browser to take certain actions when the web page first loads or when a specified event triggers the code.

61. When a user visits www.kroger.com, clicks any link or enters search terms, the user's web browser automatically sends an HTTP Request to Defendant's web server. Then, the Defendant's web server automatically returns an HTTP Response, which loads the Markup for that webpage.

62. The user does not see Defendant's Source Code, or any HTTP Requests sent in the "background" while the webpage is operating. In fact, this unseen Source Code manipulates users' browsers by secretly including the Tracking Tools' code in the webpage's Source Code, which was programmed to silently monitor and report the user's activity. For example, when the webpage containing the Meta Pixel loads into the user's browser, the Pixel code is triggered, which sends an HTTP Request to Facebook including the user's c_user id and the URL.

63. Thereafter, when an event triggers the Pixel code, the code instructs the web browser to duplicate users' Private Information (HTTP Requests) intended for Defendant and to send that Information to Facebook at the same time they are sent to Defendant. This occurs because the Pixel that was embedded in Defendant's Source Code is programmed to automatically track and transmit a user's Private Information. This occurs invisibly and without the user's knowledge.

Users Do Not Provide Informed Consent Before Their Information Is Collected and Intercepted.

64. Defendant did not ask patients, including Plaintiff and putative Class Members, whether they consented to be wiretapped via the Tracking Tools or to external sharing of their Private Information. In fact, patients were never told that their electronic communications are being wiretapped via the Tracking Tools.

65. Defendant's written policies did not adequately disclose the wiretapping and sharing of Private Information with third parties for multiple reasons.

66. As such, patients who provide their Private Information and any PII and/or PHI were not informed that Defendant would track and share their Private Information and Communications with third parties. Further, patients, including Plaintiff and Class Members, never agreed nor were given the option to agree to any such privacy policy when using the Website.

Defendant Disclosed Plaintiff's and Class Members' Private Information to Third Parties Via the Tracking Tools

67. Defendant employed the Facebook Pixel to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Facebook and other third parties.

68. Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) with Defendant and to send those communications to Facebook. These transmissions occur contemporaneously, invisibly, and without the patient's knowledge.

69. Thus, without its patients' consent, Defendant has effectively used its source code to commandeer and "bug" or "tap" its patients' computing devices, allowing Facebook and other third parties to listen in on all their communications with Defendant and thereby intercept those communications, including Private Information.

70. The Tracking Tools allow Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs. However, Defendant's Website do not rely on the Tracking Tools to function.

71. While seeking and using Defendant's services as a medical provider, Plaintiff and Class Members communicated their Private Information to Defendant via its Website.

72. Plaintiff and Class Members were not aware that their Private Information would be shared with third parties as it was communicated to Defendant because, amongst other things, Defendant did not disclose this fact.

73. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to third parties, nor did they intend for anyone other than Defendant to be a party to their communications (many of them highly sensitive and confidential) with Defendant.

74. Defendant's Tracking Tools sent non-public Private Information to third parties like Facebook, including but not limited to Plaintiff's and Class Members': (1) status as medical patients; (2) health conditions; (3) desired prescriptions; (4) desired locations or facilities where prescriptions could be purchased; (5) phrases and search queries (such as searches for providers accepting Medicare); and (6) searched and selected prescriptions at compared price points.

75. Importantly, the Private Information Defendant's Tracking Tools sent to third parties included personally identifying information that allowed those third parties to connect the Private Information to a specific patient. Information sent to Facebook was sent alongside the Plaintiff's and Class Members' Facebook ID (c_user cookie or "FID"), thereby allowing individual

patients' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts and therefore their identity.[23]

76. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including location, pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook ID to locate, access, and view the user's corresponding Facebook profile quickly and easily.

77. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented Tracking Tools that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to unauthorized third parties; and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

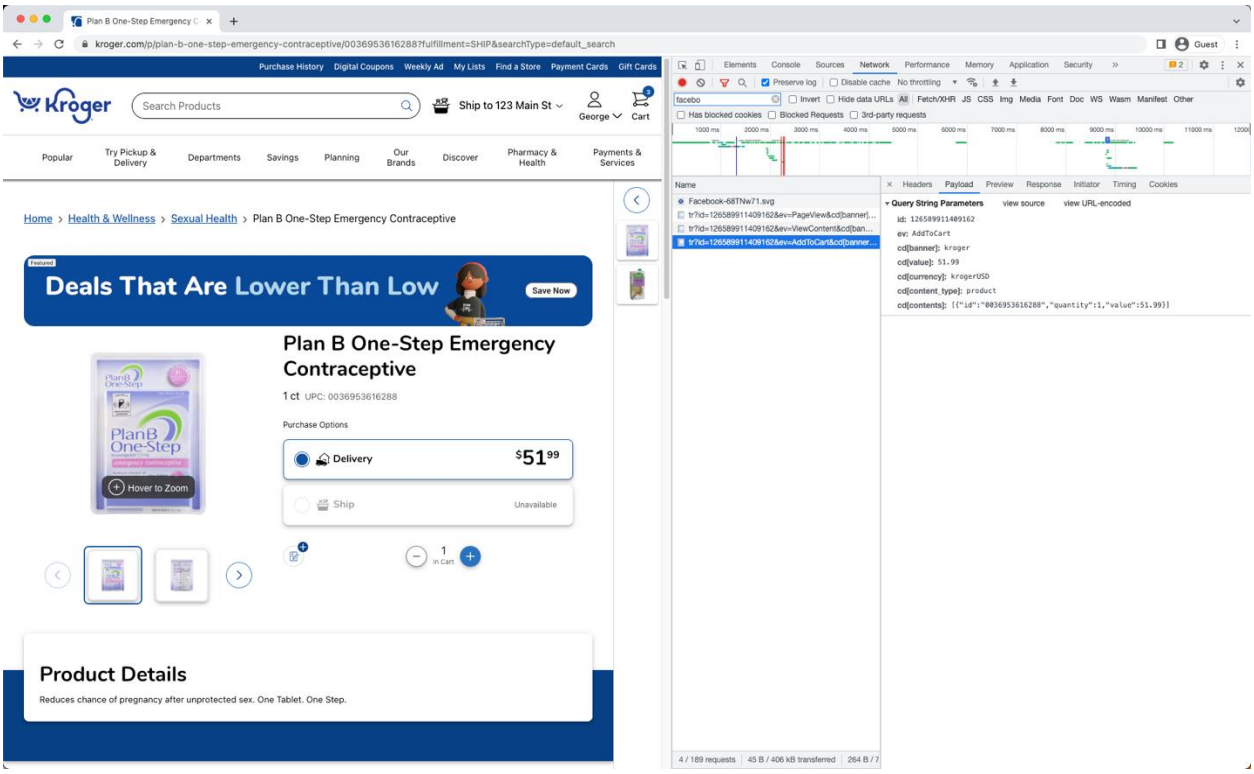
78. By installing and implementing Facebook tools, Defendant caused Plaintiff's and Class Member's communications to be intercepted by and/or disclosed to Facebook and for those communications to be personally identifiable.

79. As explained below, these unlawful transmissions are initiated by Defendant's source code concurrent with communications made via certain webpages.

[23] Defendant's Website track and transmit data via first-party and third-party cookies. The c_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

80. The example image below illustrates the point. If a patient uses the Website to search for Plan B contraceptive, a common contraceptive aid, the Website automatically shows the drug and sends the search results to Facebook.

81. Unbeknownst to ordinary patients, this webpage—which is undoubtedly used to communicate Private Information for the purpose of treating a medical condition—contains Defendant's Pixel. The image below shows the "behind the scenes" portion of the website that is invisible to ordinary users. Importantly, each entry in the column represents just one instance in which Defendant's Pixel sent this user's information to Facebook.



82. Thus, without alerting the user, Defendant's Tracking Tools send every communication the user made via the webpage to Facebook, and the images below confirm that the communications Defendant sends to Facebook contain the user's Private Information.

83. The image below is a screenshot that shows what information is sent to Facebook when the patient searches for and adds Plan B to their cart.

84. The first line of highlighted text, "id: 126589911409162" refers to Defendant's Pixel ID and confirms that Defendant has downloaded the Facebook Pixel into its Source Code for this webpage.

85. The second line of text, "ev: AddToCart," identifies and categorizes which actions the user took on the Webpage ("ev:" is an abbreviation for event, and "AddToCart" is the type of event). Thus, this identifies the user as having added the Plan B to their cart.

86. In each of the examples above, the user's website activity and the contents of the user's communications are sent to Facebook alongside their personally identifiable information. Several different methods allow marketers and third-parties to identify individual website users, but the examples above demonstrate what happens when the website user is logged into Facebook on their web browser or device. When this happens, the website user's identity is revealed via third-party cookies that work in conjunction with the Pixel. For example, the Pixel transmits the user's c_user cookie, which contains that user's unencrypted Facebook ID, and allows Facebook to link the user's online communications and interactions to their individual Facebook profile.

87. Facebook receives at least six cookies when Defendant's website transmits information via the Pixel**.**

88. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies.

89. The fr cookie contains an encrypted Facebook ID and browser identifier.[24] Facebook, at a minimum, uses the fr cookie to identify users, and this cookie can stay on a user's website browser for up to 90 days after the user has logged out of Facebook.[25]

90. The cookies listed in the two images above are commonly referred to as third-party cookies because they were "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook. Although Facebook created these cookies, Defendant is ultimately responsible for the manner in which individual website users were identified via these cookies, and Facebook would not have received this data but for Defendant's implementation and use of the Pixel throughout its website.

91. Defendant also revealed its website visitors' identities via first-party cookies such as the _fbp cookie that Facebook uses to identify a particular browser and a user:[26]

92. Importantly, the _fbp cookie is transmitted to Facebook even when the user's browser is configured to block third-party tracking cookies because, unlike the fr cookies and c_user cookie, the _fbp cookie functions as a first-party cookie—i.e. a cookie that was created and placed on the website by Defendant.[27]

93. In summation, Facebook, at a minimum, uses the fr, _fbp, and c_user cookies to link website visitors' communications and online activity with their corresponding Facebook profiles, and, because the Pixel is automatically programmed to transmit data via both first-party

---

[24] Data Protection Commissioner, Facebook Ireland Ltd: Report of Re-Audit (Sept. 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited October 10, 2023).

[25] *Cookies & other storage technologies*, FACEBOOK, https://www.facebook.com/policy/cookies/ (last visited October 11, 2023).

[26] *Id.*

[27] The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

and third-party cookies, patients' information and identities are revealed to Facebook even when they have disabled third-party cookies within their web browsers.

94. At present, the full breadth of Defendant's tracking and data sharing practices is unclear, but other evidence suggests Defendant is using additional Tracking Tools transmit its patients' Private Information to additional third parties.

95. Defendant does not disclose that the Pixel, First Party cookies, or any other Tracking Tools embedded in the Website's source code tracks, records, and transmits Plaintiff's and Class Members' Private Information to Facebook. Moreover, Defendant never received consent or written authorization to disclose Plaintiff and Class Members' private communications to Facebook.

Plaintiff Doe's Experiences

96. Plaintiff Jane Doe entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Doe disclosed her Private Information to Defendant.

97. Plaintiff Doe also maintains and regularly uses her Facebook and Instagram accounts, primarily from her mobile phone.

98. Plaintiff Doe accessed Defendant's Website via her mobile phone to receive healthcare services from Defendant, availing herself of the healthcare resources and services provided by Defendant to its customers.

99. Plaintiff Doe reasonably expected that her communications with Defendant via the website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

100. Plaintiff Doe provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

101. Indeed, Plaintiff Doe is extraordinarily protective of her Private Information, using multi-factor authentication to protect her online accounts, thoroughly destroying unnecessary physical documents with Private Information, and disabling certain features on her devices that go to far in tracking or monitoring her activity, life, or behavior.

102. As described herein, Defendant worked along with Facebook and its parent company (Meta) to intercept Plaintiff Doe's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff Doe's knowledge, consent, or express written authorization.

103. Defendant transmitted to Facebook Plaintiff Doe's Private Information, including her name, address, phone number, date of birth, and email address, along with the details (including time, place, and purpose) of medical appointments Plaintiff Doe scheduled with Defendant via Defendant's Website.

104. For example, Plaintiff Doe has used Defendant's Website annually since 2017 to schedule vaccine appointments. Defendant has transmitted to Facebook the dates and locations of these appointments, as well as the purpose of those appointments: to receive the flu vaccination and COVID-19 vaccination.

105. By doing so without Plaintiff Doe's consent, Defendant breached Plaintiff Doe's right to privacy and unlawfully disclosed Plaintiff's Private Information.

106. Plaintiff Doe suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, (iii) loss of benefit of the bargain, (iv) diminution of value of her Private Information, (v) statutory damages and (v) the continued and ongoing risk to her Private Information.

107. Plaintiff Doe has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

Third Parties Exploited and Used Plaintiff and Class Members' Private Information

108. Unsurprisingly, Meta, and other third parties do not offer the Tracking Tools to companies like Defendant solely for Defendant's benefit. "Data is the new oil of the digital economy"[28] and Meta has built market capitalizations of hundreds of billions of dollars on mining and using that "digital" oil. Thus, the large volumes of personal and sensitive health-related data Defendant provides to Meta, and other third parties are actively examined, curated, and used by those companies. The third parties acquire the raw data to transform it into a monetizable commodity, just as an oil company acquires crude oil to transform it into gasoline. Indeed, Meta offers the Pixel free of charge[29] and the price that Defendant pays for the pixel is the data that it allows Meta to collect.

109. By way of example, Meta describes itself as a "real identity platform,"[30] meaning users are allowed only one account and must share "the name they go by in everyday life."[31] To that end, when creating an account, users must provide their first and last name, date of birth, and gender.[32]

---

[28] DATA IS THE NEW OIL OF THE DIGITAL ECONOMY https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (last visited Sep. 1, 2023).

[29] FACEBOOK PIXEL: WHAT IT IS AND WHY YOU NEED IT https://seodigitalgroup.com/facebook-pixel/(last visited Sep. 1, 2023).

[30] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).

[31] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity. (last visited Sep. 1, 2023).

[32] FACEBOOK, SIGN UP, https://www.facebook.com/ (last visited Sep. 1, 2023).

110. Meta sells advertising space by emphasizing its ability to target users.[33] Meta is especially effective at targeting users because it surveils user activity both on and off its site (with the help of companies like Defendant).[34] This allows Meta to make inferences about users beyond what they explicitly disclose to Meta or via Meta's platforms, including their "interests," "behavior," and "connections."[35] Meta compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[36]

111. Advertisers can also build "Custom Audiences,"[37] which helps them reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[38] With Custom Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[39] Unlike Core Audiences, Custom Audiences and Lookalike Audiences are only available if the advertiser has sent its underlying data to Meta. This

---

[33] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706.

[34] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142. (last visited Sep. 1, 2023).

[35] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting. (last visited Sep. 1, 2023).

[36] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences. (last visited Sep. 1, 2023).

[37] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494. (last visited Sep. 1, 2023).

[38] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting. (last visited Sep. 1, 2023).

[39] Facebook, About Lookalike Audiences, https://www.facebook.com/business/help/164749007013531?id=401668390442328. (last visited Sep. 1, 2023).

data can be supplied to Meta by manually uploading contact information for customers or by utilizing Meta's "Business Tools."[40]

112. The Meta Pixel, and the Private Information mined and curated with it, is key to this business. As Meta puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Meta, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[41]

113. Meta does not merely collect information gathered by the Pixel and store it for safekeeping on its servers without ever accessing the information. Instead, in accordance with the purpose of the Pixel to allow Meta to create Core, Custom, and Lookalike Audiences for advertising and marketing purposes, Meta viewed, processed, and analyzed Plaintiff's and putative Class Members' Private Information. Upon information and belief, such viewing, processing, and analyzing was performed by computers and/or algorithms programmed and designed by Meta employees at the direction and behest of Meta, which receives over 4 petabytes of information every day and must rely on analytical tools designed to view, categorize, and extrapolate the data

[40] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; Facebook, Create a Website Custom Audience, https://www.facebook.com/business/help/1474662202748341 ?id=2469097953376494. (last visited Sep. 1, 2023).

[41] FACEBOOK, THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087. (last visited Sep. 1, 2023).

to augment human effort.[42] This process is known as data ingestion and allows "businesses to manage and make sense of large amounts of data."[43]

114. By using these tools, Meta can rapidly translate the information it receives from the Pixel in order to display relevant ads to consumers. For example, if a consumer visits a retailer's webpage and places an item in their shopping cart without purchasing it, the next time the shopper visits Facebook, an ad for that item will appear on the shopper's Facebook page.[44] This illustrates how Meta views and categorizes data as the data is received from the Pixel.

115. Moreover, even if Meta eventually deletes or anonymizes sensitive information that it receives, it must first view that information in order to identify it as containing sensitive information suitable for removal. Accordingly, there is a breach of confidentiality once the information is disclosed or received without authorization.

Defendant Was Enriched and Benefitted from the Use of the Pixel and Unauthorized Disclosures and Plaintiff's and Putative Class Members' Private Information Had Financial Value

116. The primary motivation and a determining factor in Defendant's interception and disclosure of Plaintiff's and Class Members' Private Information was to commit tortious acts as alleged herein, namely, the use of Private Information for advertising in the absence of express written consent. Defendant's further use of the Private Information after the initial interception and disclosure for marketing and revenue generation was an invasion of privacy.

---

[42] HOW DOES FACEBOOK HANDLE THE 4+ PETABYTE OF DATA GENERATED PER DAY? CAMBRIDGE ANALYTICA- FACEBOOK DATA SCANDAL https://medium.com/@srank2000/how-facebook-handles-the-4-petabyte-of-data-generated-per-day-ab86877956f4. (last visited Sep. 1, 2023).

[43] FACEBOOK DATABASE- A THOROUGH INSIGHT INTO THE DATABASES USED @ FACEBOOK https://scaleyourapp.com/what-database-does-facebook-use-a-1000-feet-deep-dive/(last visited Sep. 1, 2023).

[44] A COMPLETE GUIDE TO FACEBOOK TRACKING FOR BEGINNERS https://www.oberlo.com/blog/facebook-pixel/(last visited Sep. 1, 2023).

117. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Meta, and other third parties in the form of enhanced advertising services and more cost-efficient marketing on its platform.

118. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients.

119. By utilizing the Tracking Tools, the cost of advertising and retargeting was reduced, thereby benefiting Defendant.

120. Defendant's disclosure of Private Information also hurt Plaintiff and Class Members. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure will only increase to a total of more than $200 billion industry wide.

121. The value of health data is well known and has been reported extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[45]

122. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[46]

---

[45] HOW YOUR MEDICAL DATA FUELS A HIDDEN MULTI-BILLION DOLLAR INDUSTRY https://time.com/4588104/medical-data-industry/ (last visited Sep. 1, 2023).

[46] https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited February 16, 2023).

123. Indeed, numerous marketing services and consultants offering advice to companies on how to build their email and mobile phone lists—including those seeking to take advantage of targeted marketing—direct putative advertisers to offer consumers something of value in exchange for their personal information. "No one is giving away their email address for free. Be prepared to offer a book, guide, webinar, course or something else valuable."[47]

124. There is also a market for data in which consumers can participate. Personal information has been recognized by courts as extremely valuable. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig*., 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

125. Several companies have products through which they pay consumers for a license to track their data. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing historical information.

126. Meta also has paid users for their digital information, including browsing history. Until 2019, Meta ran a "Facebook Research" app through which it paid $20 a month for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

[47] VERO, HOW TO COLLECT EMAILS ADDRESSES ON TWITTER https://www.getvero.com/resources/twitter-lead-generation-cards/. (last visited Sep. 1, 2023).

127. Additionally, healthcare data is extremely valuable to bad actors. Health care records may be valued at up to $250 per record on the black market.[48]

The U.S. Department of Health and Human Services and Federal Trade Commission Have Warned about Use of Tracking Tools by Healthcare Providers

128. In December 2022, HHS issued a bulletin (the "HHS Bulletin") warning regulated entities like Defendant about the risks presented by the use of Tracking Tools on their websites:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[49]

In other words, the HHS has expressly stated that entities who implement Tracking Tools, such as Defendant, have violated HIPAA Rules unless they have obtained a HIPAA-complaint authorization from their patients.

129. The HHS Bulletin further warns that:

> While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.*** [50]

130. In addition, HHS and the FTC have recently issued a letter, once again admonishing entities like Defendant to stop using Tracking Tools:

---

[48] Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data, SecureLink* (June 30, 2021), https://www.securelink.com/blog/healthcare-data-new-prize-hackers.

[49] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited October 11, 2023) (emphasis added).

[50] *Id.*

> If you are a covered entity or business associate ("regulated entities") under HIPAA, you must comply with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), with regard to protected health information (PHI) that is transmitted or maintained in electronic or any other form or medium. ***The HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (e.g., tracking technology vendors) includes PHI. . .*** Even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule. . . As recent FTC enforcement actions demonstrate, it is essential to monitor data flows of health information to third parties via technologies you have integrated into your website or app. The disclosure of such information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC's Health Breach Notification Rule.[51]

Defendant Violated HIPAA Standards

131. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[52]

132. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[53]

---

[51] *Re: Use of Online Tracking Technologies*, U.S. Dept. of Health & Hum. Servs. and Fed. Trade. Comm'n (July 20, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf

[52] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

[53] HHS.gov, HIPAA For Professionals (last visited October 12, 2023), https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html.

133. The Privacy Rule broadly defines "protected health information" ("PHI") as individually identifiable health information ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

134. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

135. Under the HIPPA de-identification rule, "health information is not individually identifiable only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination'"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

a. Names;

***

H. Medical record numbers;

***

J. Account numbers;

***

M. Device identifiers and serial numbers;

> N. Web Universal Resource Locators (URLs);
>
> O. Internet Protocol (IP) address numbers; … and
>
> R. Any other unique identifying number, characteristic, or code…;and"
>
> The covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."

45 C.F.R. § 160.514.

136. The HIPAA Privacy Rule requires any "covered entity"—which includes pharmacies—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

137. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual." The statute states that a "person … shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320d-6.

138. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

139. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." In such cases, the entity that knowingly obtains individually identifiable

health information relating to an individual shall "be fined not more than $250,000, imprisoned not more than 10 years, or both."

140. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the HHS instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[54]

141. In its guidance for Marketing, the HHS further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*. (Emphasis added).[55]

142. As alleged above, there is an HHS Bulletin that highlights the obligations of "regulated entities," which are HIPAA-covered entities and business associates, when using tracking technologies.[56]

---

[54]https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited October 11, 2023).

[55]https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited Oct. 12, 2023)

[56] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

143. The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

144. Defendant's actions violated HIPAA Rules.

Patients' Expectation of Privacy

145. Plaintiff and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

146. Indeed, at all times when patients provided their Private Information to Defendant, they had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose (such as marketing), unrelated to patient care.

147. Plaintiff and Class Members would not have used the Website, would not have provided their Private Information to Defendant, and would not have paid for Defendant's healthcare services, or would have paid less for them, had they known that Defendant would disclose their Private Information to third parties.

IP Addresses Are PII

148. Defendant also disclosed and otherwise assisted third parties with intercepting patients' device IP addresses.

149. An IP address is a unique number that identifies the address of a particular device connected to the Internet, which is used to identify and route communications on the Internet.

150. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

151. For example, Facebook tracks every IP address ever associated with a Facebook user, and it uses that information to target individual homes and their occupants with advertising.

152. Under HIPAA, an IP address is considered PII:

- HIPAA defines PII to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).
- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See* also, 45 C.F.R. § 164.514(b)(2)(i)(O).

153. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

TOLLING

154. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that her Private Information was intercepted and unlawfully disclosed to third parties because Defendant kept this information secret, and the Tracking Tools were invisible.

CLASS ACTION ALLEGATIONS

155. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Nationwide Class and Ohio Subclass:

> All residents of the United States who used any website, app, or service made available by or through Kroger during the Relevant Time Period, and as a result, had their Private Information disclosed to third parties by the Tracking Tools.

> All residents of the State of Ohio who used any website, app, or service made available by or through Kroger during the Relevant Time Period, and as a result, had their Private Information disclosed to third parties by the Tracking Tools.

156. The Relevant Time Period is the longest time permitted by law.

157. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, officers, and directors, all persons who make a timely election to be excluded from the Class, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearances in this action. Plaintiff reserves the right to modify or amend the Class definition, as appropriate, during the course of this litigation.

158. **Numerosity**: The Members of the Class are so numerous that individual joinder of all Class Members is impracticable. The precise number of Class Members and their identities may be obtained from the books and records of Defendant.

159. **Commonality:** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to: (a) whether Defendant utilizes the Meta Pixel to watch in real time and intercept Defendant's Website visitors' PII and PHI; (b) whether Defendant intentionally discloses the intercepted PII and PHI of its Website users; (c) whether Defendant acquires the contents of Website users' PII and PHI without their consent; (d) whether Defendant's conduct violates state or federal privacy statutes, as cited in this Complaint.; (e) whether Plaintiff and Class Members are entitled to equitable relief; and (f) whether Plaintiff and Class Members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

160. **Typicality:** Plaintiff's claims are typical of the other Class Members' claims because, among other things, all Class Members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiff and each Member of the Class had their

communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiff and the Members of the Class typical of one another.

161. **Adequacy of Representation:** Plaintiff has fairly and adequately represented and protected the interests of the Class and will continue to do so. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the Members of the Class, and they have the resources to do so. Neither Plaintiff nor her counsel have any interest adverse to the interests of the other Members of the Class.

162. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all Members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

163. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each Member of the Class.

If Defendant intercepted Plaintiff's and Class Members' Website Communications, then Plaintiff and each Class Member suffered damages by that conduct.

164. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Kroger's records or Meta's records.

CLAIMS FOR RELIEF

COUNT I
Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2511(1) ("ECPA")
(On Behalf of Plaintiff and the Nationwide Class)

165. Plaintiff repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

166. The ECPA protects both the sending and receipt of communications.

167. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral, or electronic communication is intercepted.

168. A violation of the ECPA occurs where any person "**intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept**, any . . . **electronic communication**" or "intentionally discloses, or endeavors to disclose, to any other person the contents of any . . . electronic communication, **knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication**" or "intentionally uses, or endeavors to use, the contents of any . . . electronic communication, knowing or having reason to know that the information was **obtained through the [unlawful] interception of a[n] . . . electronic communication**." 18 U.S.C. §§ 2511(1)(a), (c)-(d)(emphasis added).

169. "Intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

170. "Electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

171. "Contents" includes "any information relating to the substance, purport, or meaning" of the communication at issue. 18 U.S.C. § 2510(8).

172. By utilizing and embedding the Tracking Tools on its Website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a). Whenever Plaintiff and Class Members interacted with Defendant's Website, Defendant through the Tracking Tools' source code it embedded and ran on its Website, contemporaneously and intentionally intercepted, and endeavored to intercept Plaintiff's and Class Members' electronic communications without authorization or consent.

173. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to Meta, while knowing or having reason to know that Private Information protected by HIPAA and other statutory and common law was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

174. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the

Private Information protected by HIPAA and other statutory and common law was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

175. Defendant intentionally used the wire or electronic communications for the purpose of sharing and disclosing Private Information to third parties in violation of HIPAA and other statutory and common law. Defendant could not otherwise have made such disclosures without using the hidden Tracking Tools to surreptitiously disclose the Private Information without obtaining patient authorization or consent. Defendant specifically used the Pixel to track and utilize Plaintiff's and Class Members' Private Information for financial gain and to increase its profit margins by violating HIPAA and other statutory and common law as described herein.

176. Defendant was not acting under color of law to intercept Plaintiff's and Class Members' wire or electronic communication.

177. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading their privacy via the Tracking Tools.

178. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

179. Unauthorized Purpose – Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, violation of HIPAA, CIPA, CMIA, UCL, WESCA, FSCA, and the common law, including invasion of privacy. The ECPA provides that a "party to the communication" may liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

180. Defendant is not a party to the communication based on its unauthorized duplication and transmission of communications with Plaintiff and Class Members. *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020) (an entity's simultaneous, unknown duplication and forwarding of GET requests made to a web page's server does not qualify for the party exemption, because holding otherwise "would render permissible the most common methods of intrusion, allowing the exception to swallow the rule"). However, even assuming Defendant is a party, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiff's and Class Members' Private Information does not qualify for the party exemption.

181. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiff's and Class Members' communications about their Private Information on its Website, because it used its participation in these communications to improperly share Plaintiff and Class Members' Private Information with third parties that did not participate in these communications, that Plaintiff and Class Members did not know was receiving their Private Information, and that Plaintiff and Class Members did not consent to receive this information, for the purpose of committing criminal or tortious acts as described above.

182. As a result of Defendant's violation of the ECPA, Plaintiff and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorneys' fees and costs.

COUNT II
Breach of Confidence
(On Behalf of Plaintiff and the Nationwide Class)

183. Plaintiff incorporates all prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

184. Medical providers in Ohio have a duty to their patients to keep Private Information confidential and to not disclose Private Information to third parties without the patient's informed consent or other applicable legal privilege entitling them to do so.

185. Plaintiff and Class Members had reasonable expectations of privacy when interacting with Defendant through its digital properties, including communications made on the Website, in virtue of this well-known duty of confidentiality incumbent upon medical providers.

186. Contrary to its duty as a medical provider, Defendant deployed the Tracking Tools to secretly record and transmit nonpublic Private Information to third parties as described throughout this Complaint without patient authorization or consent.

187. The Private Information that Defendant transmitted to third parties without authorization was learned within a physician-patient relationship.

188. Defendant's breaches of confidence were committed negligently, recklessly, and/or intentionally.

189. Defendant's breaches of confidence were a direct and proximate cause of several injuries suffered by Plaintiff and Class Members, including, but not limited to, losses of privacy, interference with confidential relationships, diminished value of Private Information, and the lost benefit of their bargains with Defendant. Plaintiff and Class Members seek compensatory damages in an amount to be proved at trial. In the alternative, Plaintiff and Class Members seek nominal damages.

COUNT III
Invasion of Privacy - Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Nationwide Class)

190. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

191. The Private Information of Plaintiff and Class Members is private, confidential, and not intended to be shared with third parties absent authorization.

192. Plaintiff and Class Members had a legitimate expectation of privacy regarding their Private Information and communications with Defendant, and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

193. Defendant owed a duty to Plaintiff and Class Members to keep their Private Information and communications confidential.

194. Defendant's conduct constitutes a physical or sensory intrusion on Plaintiff's and Class Members' privacy because Defendant installed the Tracking Tools on its Website for the purpose of secretly recording the activity on Plaintiff's and Class Members' browsers and then transmitting the Private Information learned from this activity to third parties for commercial purposes without authorization or consent.

195. The secret recording and transmission of Plaintiff's and Class Members' Private Information and communications to third parties for commercial purposes without authorization or consent is highly offensive and/or outrageous to a reasonable person.

196. Defendant's conduct constitutes an interference with Plaintiff's and Class Members' interest in solitude or seclusion.

197. Defendant's invasions of privacy were a direct and proximate cause of several injuries suffered by Plaintiff and Class Members, including, but not limited to, losses of privacy,

interference with confidential relationships, diminished value of Private Information, and the lost benefit of their bargains. Plaintiff and Class Members seek compensatory damages in an amount to be proved at trial. In the alternative, Plaintiff and Class Members seek nominal damages.

COUNT IV
Breach of Implied Contract
(on behalf of Plaintiff and the Nationwide Class)

198. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

199. As a condition of utilizing Defendant's Website and receiving services from Defendant's healthcare facilities and professionals, Plaintiff and Class Members provided their Private Information and compensation for their medical care.

200. When Plaintiff and Class Members provided their Private Information to Defendant, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

201. Plaintiff and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

202. Plaintiff and Class Members would not have retained Defendant to provide healthcare services in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

203. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information without consent to third parties for commercial purposes.

204. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein, including but not limited to the loss of the benefit of their bargain and diminution in value of Private Information.

205. Defendant's breaches of implied contract were a direct and proximate cause of several injuries suffered by Plaintiff and Class Members, including, but not limited to, losses of privacy, interference with confidential relationships, diminished value of Private Information, and the lost benefit of their bargains with Defendant. Plaintiff and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract. In the alternative, Plaintiff and Class Members seek nominal damages.

COUNT V
Unjust Enrichment
(On behalf of Plaintiff and the Nationwide Class)

206. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

207. This claim is brought in the alternative to breach of implied contract.

208. Defendant benefits from the use of Plaintiff's and Class Members' Private Information and unjustly retained those benefits at their expense.

209. Plaintiff and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation to exceed the limited authorization and access to that information which was given to Defendant.

210. Defendant exceeded any authorization given and instead consciously disclosed and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

211. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

212. The benefits that Defendant derived from Plaintiff and Class Members was not offered by Plaintiff and Class Members gratuitously and rightly belongs to Plaintiff and Class Members. It would be against equity and good conscience for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

213. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT VI
Negligence
(On behalf of Plaintiff and the Nationwide Class)

214. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

215. This claim is brought in the alternative to breach of confidence (Biddle).

216. Defendant owed Plaintiff and Class Members a duty to keep their Private Information completely confidential, and to safeguard sensitive personal and medical information.

217. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

218. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed its Tracking Tools to disclose and transmit to third parties

Plaintiff's and Class Members' communications with Defendant, including Private Information and the contents of such information.

219. These disclosures were made without Plaintiff's or Class Members' knowledge, consent, or authorization, and were unprivileged.

220. Defendant's negligence was a direct and proximate cause of several injuries suffered by Plaintiff and Class Members, including, but not limited to, losses of privacy, interference with confidential relationships, diminished value of Private Information, and the lost benefit of their bargains with Defendant. Plaintiff and Class Members seek compensatory damages in an amount to be proved at trial. In the alternative, Plaintiff and Class Members seek nominal damages.

COUNT VII
Breach of Fiduciary Duty
(on behalf of Plaintiff and the Nationwide Class)

221. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

222. This claim is brought in the alternative to breach of confidence (Biddle).

223. Defendant has a fiduciary duty to act primarily for the benefit of its patients, including Plaintiff and Class Members by: (1) safeguarding Plaintiff's and Class Members' Private Information; (2) timely notifying Plaintiff and Class Members of disclosure of their Private Information to unauthorized third parties; and (3) maintaining complete and accurate records of what patient information (and where) Defendant did and does store and disclose.

224. Defendant breached its fiduciary duty to Plaintiff and Class Members by failing to protect and/or intentionally disclosing Plaintiff's and Class Members' Private Information to third parties without authorization or consent.

225. Defendant's breach of fiduciary duty is evidenced by its failure to comply with federal and state privacy regulations, including:

a. By failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

b. By failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

c. By failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4);

d. By failing to obtain satisfactory assurances, including in writing, that its business associates and/or subcontractors would appropriately safeguard Plaintiff's and Class Members' PHI;

e. By failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. By failing to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network in violation of 45 C.F.R. § 164.312(e)(1);

g. By impermissibly and improperly using and disclosing Private Information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq., 45 C.F.R. § 164.508, et seq., and R.C. 3798.04, et seq.;

h. By failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. By failing to comply with R.C. 3798.04 regarding the use or disclosure of protected health information.

226. Defendant's breaches of fiduciary duty were a direct and proximate cause of several injuries suffered by Plaintiff and Class Members, including, but not limited to, losses of privacy, interference with confidential relationships, diminished value of Private Information, and the lost benefit of their bargains. Plaintiff and Class Members seek compensatory damages in an amount to be proved at trial. In the alternative, Plaintiff and Class Members seek nominal damages.

COUNT VIII
Interception and Disclosure of Electronic Communications in Violation of R.C. 2933.52 (on behalf of Plaintiff and the Ohio Subclass)

227. Plaintiff repeats and re-alleges each and every paragraph in the Complaint as if fully set forth herein.

228. Plaintiff brings this claim on behalf of herself and all members of the Class.

229. All conditions precedent to this action have been performed or have occurred.

230. R.C. 2933.52(B)(4) provides that it is unlawful for a person not acting under law to intercept an electronic communication "for the purpose of committing a criminal offense or tortious act in violation of the laws or Constitution of the United States or this state for the purpose of committing any other injurious act."

231. Defendant intercepted Plaintiff's and Class Members' electronic communications for the purpose of committing multiple tortious acts, including, but not limited to, the criminal and tortious acts as detailed throughout the complaint.

232. For example, Defendant intercepted Plaintiff's and Class Members' electronic communications for the purpose of disclosing those communications to Facebook without the knowledge, consent, or written authorization of Plaintiff or Class Members. The disclosure of Plaintiff's and Class Members' Personal Health Information to Facebook without consent or proper authorization is an illegal or tortious act that violates multiple laws, including (but not limited to) 42 U.S.C. § 1320d-6, 15 U.S.C. 45, R.C. 3798.04, R.C. 3798.03(2), 45 CFR § 164.508(a)(1), R.C. 1345.02(A), R.C. 1345.03(A), and R.C. 1347.05(g). Defendant's misconduct accordingly falls within the ambit of Ohio's wiretapping statute.

233. Further, as set forth above, Defendant's interception of Plaintiff's and Class Members' electronic communications for the purpose of disclosing their Private Information to Facebook is also a tortious act that constitutes a breach of the fiduciary duty of confidentiality owed by doctors and hospital systems to their patients as set forth by the Ohio Supreme Court in *Biddle v. Warren General Hospital*, 86 Ohio St. 3d 395, 401 (1999).

234. Any person whose wire, oral, or electronic communications are intercepted, disclosed, or intentionally used in violation of the Wiretap Act may bring a civil action to recover from the person or entity that engaged in the violation. R.C. 2933.65.

235. Defendant violated the Ohio Wiretap Act by intercepting Plaintiff's and Class Members' electronic communications in violation of R.C. 2933.52(A)(1).

236. Defendant separately violated the Ohio Wiretap Act by using the contents of a Plaintiff's and Class Members' electronic communications, knowing or having reason to know,

that the contents were obtained through the interception of an electronic communication in violation of R.C. 2933.52(A)(3). Specifically, Defendant knowingly used the contents of Plaintiff's and Class Members' electronic communications to barter and/or sell that information to Facebook in return for access to the Tracking Tools.

237. Defendant qualifies as a person under the statute.

238. Ohio law defines "electronic communications" to mean "the transfer of a sign, signal, writing, image, sound, datum, or intelligence of any nature that is transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system." R.C. 2933.51(N). Plaintiff's and Class Members' communications with Defendant constitute "electronic communications" under Ohio law because each communication is made using personal computing devices (e.g., computers, smartphones, tablets) that send and receive communications in whole or in part through the use of facilities used for the transmission of communications aided by wire, cable, or other like connections.

239. Defendant engaged in and continues to engage in interception by aiding others (including Facebook) to secretly record the contents of Plaintiff's and Class Members' wire communications.

240. The intercepting devices used in this case include, but are not limited to:

a. Plaintiff's and Class Members' personal computing devices;

b. Plaintiff's and Class Members' web browsers;

c. Plaintiff's and Class Members' browser-managed files;

d. The Tracking Tools;

e. Facebook's Meta Pixel;

f. Internet cookies;

g. Defendant's computer servers;

h. Third-party source code utilized by Defendant; and

i. Computer servers of third parties (including Facebook) to which Plaintiff's and Class Members' communications were disclosed.

241. "Contents" under the Act, when used with respect to any electronic communication, includes "any information concerning the substance, purport, or meaning of the communication." R.C. 2933.51(G).

242. Defendant aided in, and continues to aid in, the interception of contents in that the data from the communications between Plaintiff and/or Class Members and Defendant that were redirected to and recorded by the third parties include information which identifies the parties to each communication, their existence, and their contents.

243. Defendant aided in the interception of "contents" in at least the following forms:

a. The parties to the communications;

b. The precise text of patient search queries;

c. PII such as patients' IP addresses, Facebook IDs, browser fingerprints, and other unique identifiers;

d. The precise text of patient communications about specific doctors;

e. The precise text of patient communications about specific medical conditions;

f. The precise text of patient communications about specific treatments;

g. The precise text of patient communications about scheduling appointments with medical providers;

h. The precise text of patient communications about billing and payment;

i. The precise text of specific buttons on Defendant's website(s) that patients

click to exchange communications, including Log-Ins, Registrations, Requests for Appointments, Search, and other buttons;

j. The precise dates and times when patients click to Log-In on Defendant's Website;

k. The precise dates and times when patients visit Defendant's Website;

l. Information that is a general summary or informs third parties of the general subject of communications that Defendant sends back to patients in response to search queries and requests for information about specific doctors, conditions, treatments, billing, payment, and other information; and

m. Any other content that Defendant has aided third parties in scraping from webpages or communication forms at web properties.

244. Plaintiff and Class Members reasonably expected that their Private Information was not being intercepted, recorded, and disclosed to Facebook or other third-party advertising companies.

245. No legitimate purpose was served by Defendant's willful and intentional disclosure of Plaintiff's and Class Members' Private Information to Facebook and similar third-party advertising companies. Neither Plaintiff nor Class Members consented to the disclosure of their Private Information by Defendant to these third parties. Nor could they have consented, given that Defendant never sought Plaintiff's or Class Members' consent, or even told visitors to its website that their every interaction was being recorded and transmitted to Facebook and other third parties via Tracking Tools so that these third parties could monetize their Private Information.

246. Plaintiff's and Class Members' electronic communications were intercepted during transmission, without their consent, for the unlawful and/or wrongful purpose of monetizing their

Private Information, including using their sensitive medical information to develop marketing and advertising strategies.

247. Under the Wiretapping Act, aggrieved persons are entitled to recover actual damages, but not less than liquidated damages computed at the rate of one hundred dollars a day for each day of the violation or ten thousand dollars whichever is greater, punitive damages, and reasonable attorney's fees and other litigation costs. R.C. 2933.65.

248. In addition to statutory damages, Defendant's breach caused Plaintiff and Class Members the following damages:

a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

b. Defendant eroded the essential confidential nature of the doctor-patient relationship;

c. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

d. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

e. Defendant's actions diminished the value of Plaintiff's and Class Members' personal information.

249. Plaintiff and Class Members have been irreparably harmed by the loss of their privacy. Plaintiff and Class Members will continue to face a substantial risk of irreparable harm from Defendant's actions if not enjoined. Defendant is a major medical provider. Depending on

the type and severity of future illness or injury, Plaintiff and Class Members may be required to seek Defendant's medical services. An injunction would serve the public interest because Plaintiff and other Ohio residents should not be forced to choose between receiving necessary medical services and maintaining the confidentiality of their Private Information.

250. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

REQUEST FOR RELIEF

Plaintiff, individually and on behalf of the other Members of the proposed Class, respectfully requests that the Court enter judgment in favor of Plaintiff and the Class and against Defendant as follows:

A. Certifying the Class and appointing Plaintiff as Class Representative;

B. Appointing Plaintiff's counsel as Class Counsel;

C. Declaring that Defendant's past conduct was unlawful, as alleged herein;

D. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;

E. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;

F. Awarding Plaintiff and Class Members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

G. Awarding Plaintiff and Class Members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and Class Members reasonable attorneys' fees, costs, and litigation expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Class, demands a trial by jury of any and all issues in this action so triable of right.

Dated: November 10, 2023

Respectfully submitted,

/s/ Terence R. Coates
Terence R. Coates (0085579) – **Trial Attorney**
Dylan J. Gould (0097954)
Spencer D. Campbell (103001)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com
scampbell@msdlegal.com

Gary M. Klinger (*pro hac vice forthcoming*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
221 W. Monroe Street, Suite 2100
Chicago, IL 60606
gklinger@milberg.com

Attorneys for Plaintiff and Class Members